LECTURE 25: RADICAL EXTENSIONS & SOLVABILITY

The impossibility of solving the 5^{th} order polynomial equation in terms of it coefficients and a simple formula involving radicals and arithmetic is the problem which motivated Galois to discover group theoretic arguments... We now return to this problem, first we must study the easiest n^{th} order poly. eq^n; $x^n = a$. Actually, we already did in §13.6 when we studied cyclotomic fields...

Def^n/ The extension K/F is said to be cyclic if it is Galois with a cyclic Galois group

Simple radical extensions are obtained by adjoining to F an n^{th} root of some $a \in F$. Since solutions of $x^n - a = 0$ * include $\sqrt[n]{a}$ ← any particular sol^n to * and $\sqrt[n]{a}\,\zeta_n^k$ for $k = 1, 2, \ldots, n-1$, this means that if F contains the n^{th} roots of unity then $F(\sqrt[n]{a})$ behaves "nicely"

E1 $x^2 - p$ where p prime, $\mathbb{Q}(\sqrt{p})$ is splitting field for $x^2 - p$ and $\zeta_2 = -1 \in \mathbb{Q}$. Also, $\mathrm{Gal}(\mathbb{Q}(\sqrt{p})/\mathbb{Q}) = \{1, \sigma\}$ where $\sigma(a + b\sqrt{p}) = a - b\sqrt{p}$

Cyclic group, order 2 $\therefore$ $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ cyclic.

E2 $x^3 - 2 \in \mathbb{Q}(i\sqrt{3}) = F$ then $\zeta_3 = \frac{-1 + i\sqrt{3}}{2} \in \mathbb{Q}(i\sqrt{3})$ hence $(\mathbb{Q}(i\sqrt{3}))(\sqrt[3]{2})$ splits $x^3 - 2$ and I suspect $\left[\mathbb{Q}(i\sqrt{3}, \sqrt[3]{2}) : \mathbb{Q}(i\sqrt{3})\right] = 3$ with $\mathrm{Gal}(\mathbb{Q}(i\sqrt{3}, \sqrt[3]{2})/\mathbb{Q}(i\sqrt{3})) \cong \mathbb{Z}_3$.

PROPOSITION (36)

Let F be a field of characteristic not dividing n which contains the n^{th} roots of unity. Then the extension $F(\sqrt[n]{a})$ for $a \in F$ is cyclic over F of degree dividing n

Proof: $K = F(\sqrt[n]{a})$ is a splitting field for $x^n - a \in F[x]$ provided F contains the n^{th} roots of unity. Thus K/F is Galois. We know $\sigma \in \text{Aut}(K/F)$ permutes roots of $x^n - a$ thus $\exists\, \zeta_\sigma$ an n^{th} root of unity for which

$$\sigma(\sqrt[n]{a}) = \zeta_\sigma \sqrt[n]{a}$$

Consequently, $\sigma \xrightarrow{\psi} \zeta_\sigma$ gives map from $\text{Gal}(K/F)$ to $\mu_n \subset F$ (by assumption F contains n^{th} roots of unity). Observe,

actually, a homomorphism.

$$\sigma\tau(\sqrt[n]{a}) = \sigma(\zeta_\tau \sqrt[n]{a})$$
$$= \zeta_\tau \sigma(\sqrt[n]{a})$$
$$= \zeta_\tau \zeta_\sigma \sqrt[n]{a} \quad \therefore \underline{\zeta_{\sigma\tau} = \zeta_\sigma \zeta_\tau}.$$

The kernel $\ker(\psi) = \{1\}$ since any map in $\ker\psi$ must fix $\sqrt[n]{a}$ and only the identity automorphism does that.

Hence $\psi: \text{Gal}(K/F) \longrightarrow \mu_n$ gives an isomorphism onto $\psi(\text{Gal}(K/F)) \leq \mu_n \Rightarrow \text{Gal}(K/F)$ is isomorphic to subgroup of $\mu_n \Rightarrow$ $\text{Gal}(K/F)$ is isomorphic to subgroup of the cyclic group of order n

$\Rightarrow |\text{Gal}(K/F)| \mid n$ and $\text{Gal}(K/F)$ is cyclic. //

Def? Suppose K is a cyclic extension of degree n over field F with $\mathrm{char}(F) \nmid n$ and $\mu_n \subset F$. Let $\langle \sigma \rangle = \mathrm{Gal}(K/F)$, that is σ is a generator for $\mathrm{Gal}(K/F)$. Then for $\alpha \in K$ and any $\zeta \in \mu_n$ define the Lagrange resolvent $(\alpha, \zeta) \in K$ by

$$(\alpha, \zeta) = \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha)$$

Let's calculate $\sigma(\alpha, \zeta)$, notice $\sigma(\zeta) = \zeta$ as $\zeta \in F$

$$\begin{aligned}
\sigma(\alpha, \zeta) &= \sigma(\alpha) + \sigma(\zeta\sigma(\alpha)) + \sigma(\zeta^2\sigma^2(\alpha)) + \cdots + \sigma(\zeta^{n-1}\sigma^{n-1}(\alpha)) \\
&= \sigma(\alpha) + \zeta\sigma^2(\alpha) + \zeta^2\sigma^3(\alpha) + \cdots + \zeta^{n-1}\sigma^n(\alpha) \\
&= \sigma(\alpha) + \zeta\sigma^2(\alpha) + \zeta^2\sigma^3(\alpha) + \cdots + \zeta^{-1}\alpha \\
&= \zeta^{-1}\left(\alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha)\right) \\
&= \zeta^{-1}\,(\alpha, \zeta)
\end{aligned}$$

$\zeta^n = 1$, $\sigma^n = 1$, $\sigma \in \mathrm{Gal}(K/F)$, $|\sigma| = n$.

Therefore,

$$\sigma(\alpha, \zeta)^n = (\zeta^{-1})^n\,(\alpha, \zeta)^n = (\alpha, \zeta)^n$$

It follows $(\alpha, \zeta)^n$ is fixed by $\mathrm{Gal}(K/F) \therefore \boxed{(\alpha, \zeta)^n \in F}$

Use LI of automorphisms $1, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ to see $\exists \alpha \in K$ with $(\alpha, \zeta) = \alpha + \zeta\sigma(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha) \neq 0$. Then

$$\sigma^j(\alpha, \zeta) = \zeta^{-j}(\alpha, \zeta) \quad \text{for } j = 0, 1, \ldots$$

thus σ^j does not fix (α, ζ) for any $j < n$. It follows (α, ζ) cannot be in any subfield (proper) of $K \therefore K = F((\alpha, \zeta))$

Furthermore, $(\alpha, \zeta)^n = a \in F \therefore K = F(\sqrt[n]{a})$.

PROPOSITION (37)

Any cyclic extension of degree n over a field F of $\text{char}(F) \nmid n$ with $\mu_n \subset F$ is of the form $F(\sqrt[n]{a})$ for some $a \in F$.

The exponent of a group G is n if $g^n = 1$ for every $g \in G$. For instance, $U(\mathbb{Z}_{11} \times \mathbb{Z}_7) \cong \mathbb{Z}_{10} \times \mathbb{Z}_6$ has $n = 30$.

More to the discussion of extensions,

$$F(\sqrt[n]{a_1}, \sqrt[n]{a_2}, \ldots, \sqrt[n]{a_k}) = K$$

gives abelian extension of F with $\text{Gal}(K/F)$ a group with exponent n. Dummit & Foote, pg. 626 claims every abelian ext. of exponent n is of this form.

$\text{Def}^n / (F^\times)^n = \{a^n \mid a \in F^\times\}$ n^{th} power subgroup of $F^\times$

Then $F^\times / (F^\times)^n$ is abelian group of exponent n.

CLAIM: $\text{Gal}(K/F)$ isomorphic to group generated in $F^\times/(F^\times)^n$ by elements $a_1, a_2, \ldots, a_k$ and any two extensions like K are equal iff their associated subgroups in $F^\times/(F^\times)^n$ are equal. Thus the finitely generated subgroups of $F^\times/(F^\times)^n$ classify abelian extensions of exponent n over fields containing μ_n and having $\text{char}(F) \nmid n$. (§17.3 for more on Kummer Theory)

Let us now focus on char(F) = 0

Def'n (1.) An element α which is algebraic over F can be expressed by radicals or solved for in terms of radicals if $\alpha \in K$ which can be obtained by a succession of simple radical extensions

$$F = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_s = K$$

where

$$K_{i+1} = K_i\left(\sqrt[n_i]{a_i}\right)$$

for some $a_i \in K_i$, $i = 0, 1, \ldots, s-1$.

Here $\sqrt[n_i]{a_i}$ denotes some root of the polynomial $x^{n_i} - a_i$. We call such K a root extension of F.

(2.) A polynomial $f(x) \in F[x]$ can be solved by radicals if all its roots can be solved for in terms of radicals.

E3 $K_0 = \mathbb{Q}$ (see PROP 29)

$K_1 = K_0(\sqrt{a_0})$ $\quad a_0 = 17$

$K_2 = K_1(\sqrt{a_1})$ $\quad a_1 = 2(17 - \sqrt{17})$

$K_3 = K_2(\sqrt{a_2})$ $\quad a_2 = 2(17 + \sqrt{17})$

$K_4 = K_3(\sqrt{a_3})$ $\quad a_3 = 17 + 3\sqrt{17} - \sqrt{2(17-\sqrt{17})} - 2\sqrt{2(17+\sqrt{17})}$

This underlies the compass-straightedge construction of the reg. 17-gon

Gauss in 1796, age 19 to construct $\mathbb{Q}(\sqrt[17]{1})$ via subfields of degrees 2, 4, 8 and 16 ... (page 602 of §14.5 Dummit & Foote for more)

Lemma (38)

If α is contained in a root extension K then α is in a root extension which is Galois over F and where each extension K_{i+1}/K_i is cyclic.

Proof: Suppose L is the "Galois closure" of K over F. For any $\sigma \in Gal(L/F)$ we have the chain of subfields,

$$F = \sigma K_0 \subset \sigma K_1 \subset \cdots \subset \sigma K_i \subset \sigma K_{i+1} \subset \cdots \subset \sigma K_s = \sigma K,$$

where $\sigma K_{i+1}/\sigma K_i$ is a simple radical extension (since it is generated by $\sigma(\sqrt[n_i]{a_i})$ which is root of the eqn $x^{n_i} - \sigma(a_i)$ over $\sigma(K_i)$). We claim the composite of two root extensions is once more a root extension. Then it follows the composite of all the conjugate fields $\sigma(K)$ for $\sigma \in Gal(L/F)$ is a root extension. But, this composite field is how we form L. Hence α is contained in root extension which is Galois over F. Next adjoin the $(n_i)^{th}$ roots of unity for all the roots $\sqrt[n_i]{a_i}$ of the simple radical extensions forming K/F, use F' for extended F,

$$F \subseteq F' = F'K_0 \subset F'K_1 \subseteq \cdots \subseteq F'K_i \subset F'K_{i+1} \subseteq \cdots \subseteq F'K_s = F'K$$

Then $F'K$ is Galois extension of F and the above chain of subfields establishes Lemma (38). //

(See p. 628 of Dummit & Foote for a few more details)